IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	**8:15CR172**
	)	
V.	)	
	)	
MIKEL MILLER,	)	**FINDINGS AND**
	)	**RECOMMENDATION**
Defendant.	)	
	)	

This matter is before the Court on Defendant's Motion to Suppress, Application for Franks Hearing, and Request for Evidentiary Hearing and Oral Argument. (Filing 33.) For the reasons set forth below, the undersigned will recommend to Senior District Court Judge Lyle Strom that Defendant's Motion be denied in its entirety.

BACKGROUND

Google, an electronic communication service provider, scans files sent through its network to search for contraband images of child pornography. Once it finds a contraband image, Google, in compliance with the reporting requirements of 18 U.S.C. § 2258A, provides a report to the National Center for Missing and Exploited Children ("NCMEC"), which, in turn, creates a report called a CyberTipline Report about the specific information provided by Google.

On or about December 7, 2014, the NCMEC received a CyberTip from Google, reporting that a Google email address ("gmail address"), mikemillerbi@gmail.com, had uploaded an image consistent with child pornography. The NCMEC referred the matter to the Nebraska State Patrol based on information that the internet protocol ("IP") address associated with the upload was located in Fremont, Nebraska. Through further investigation, officials determined that the IP address was registered to Robin Martens ("Martens") at 224 N. Maple Street, Fremont, Nebraska.

On December 24, 2014, the NCMEC received another CyberTip from Google, indicating that a gmail address, terrimillerbu@gmail.com, uploaded child pornography. The NCMEC reviewed the image and IP addresses associated with the gmail account and image upload. The IP address captured for the image belonged to Hosted Data Solutions. An additional IP address associated with the gmail account was registered to Martens at 224 N. Maple Street, Fremont, Nebraska. The NCMEC report also listed several other IP addresses associated with the gmail account, but investigation revealed that they were mobile services IP addresses.

On January 5, 2015, the NCMEC received a CyberTip from Google, indicating that a gmail user, mikeltmillerbu@gmail.com, uploaded an image of child pornography. The IP address captured for the image upload was registered to Martens at 224 N. Maple Street, Fremont, Nebraska. The report also listed several mobile services IP addresses associated with the gmail account.

The NCMEC received another CyberTip from Google on February 25, 2015, indicating that a gmail user, mikeltmiller2@gmail.com, uploaded an image of child pornography. The IP address associated with the image upload was registered to Martens at 224 N. Maple Street, Fremont, Nebraska. The NCMEC report also listed several additional IP addresses associated with the gmail account. Investigation revealed that these additional IP addresses were mobile services addresses.

Based on the different gmail accounts being connected to the IP address registered to Martens, Homeland Security Investigations Special Agent Eric Cardiel ("Cardiel") applied for and received a search warrant for the residence at 224 N. Maple Street, Fremont, Nebraska. The affidavit used to support the application for the search warrant did not include information about the other IP addresses listed in the CyberTipline Reports.

Cardiel also sought and received a search warrant for a residence located at 750 E. 2nd, #1, Fremont, Nebraska. Cardiel requested a search warrant for this second residence because an IP address registered to that location was also identified in a CyberTipline Report as being associated with a gmail account that uploaded an image of child pornography. The IP address belonged to Patrick Heise, a registered sex offender in Nebraska.

Homeland Security Investigations ("HSI") executed a search warrant on 224 N. Maple Street, Fremont, Nebraska on April 21, 2015. Agents seized three cell phones, a tower computer, three flash drives and other items. During the execution of the search warrant, HSI encountered Defendant who, after waiving his *Miranda* rights, stated that he had lived in the residence with Martens for two years. Miller told HSI agents that they would find child pornography on thumb drives seized from his bedroom. He also stated that he would use the internet connection associated with apartments across the street from his house. The residence across the street was 750 E.2d Street, #1, Fremont, Nebraska, where HSI had also executed a search warrant.

Defendant was subsequently charged with receipt and distribution of child pornography (Count I) and possession of child pornography (Court II). On August 10, 2015, Defendant filed a motion requesting a *Franks* hearing and suppression of evidence found during the execution of the search warrant, including all statements taken from him.

DISCUSSION

I. Request for Franks Hearing

Defendant contends a *Franks* violation occurred because Cardiel omitted material facts from the affidavit used to obtain the search warrant. In particular, Defendant complains that Cardiel did not include information regarding other locations and IP addresses associated with the gmail addresses in the NCMEC CyberTipline Reports. Defendant argues that the large number of different IP addresses should have been disclosed so the Court could make a more reasoned decision about probable cause.

To void a search warrant under *Franks v. Delaware*, 438 U.S. 154 (1978), a defendant must make a substantial preliminary showing that (1) the affiant included in the warrant affidavit a false statement knowingly and intentionally, or with reckless disregard for the truth, and (2) the affidavit's remaining content is insufficient to establish probable cause. *Id*. Omissions from an affidavit can likewise vitiate a warrant if the defendant proves "first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted

information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

The undersigned finds that the affidavit does not contain any intentionally false statements or that the affidavit's remaining content is insufficient to establish probable cause. Likewise, the undersigned concludes that no material information was omitted from the affidavit or that this omitted information would impact probable cause. It is undisputed that Cardiel did not include information about other IP addresses contained in the NCMEC CyberTipline Reports in the affidavit. However, the additional IP addresses, unlike the IP addresses discussed in the affidavit, were mobile IP addresses. Mobile IP addresses are IP address locations that a mobile phone or other wireless device can connect to. Unlike the IP addresses mentioned in Cardiel's affidavit, a mobile IP address alone does not provide information about a specific user's location. Information about the mobile IP addresses would have only provided information that the gmail account user was accessing his or her account through a wireless connection on a wireless enabled device. Therefore, any omitted information regarding the additional IP addresses would not have impacted the sufficiency of probable cause. Also, the fact that the IP address registered to Martens had come up several times in CyberTipline Reports makes it highly likely that a judge would have found sufficient probable cause to issue the warrant even had information about the other IP addresses been included in the affidavit. Accordingly, Defendant's request for a *Franks* hearing should be denied.

2. Motion to Suppress

Defendant contends that his Fourth Amendment rights were violated when Google searched his gmail accounts without a warrant. Defendant argues that due to this constitutional violation, all evidence obtained directly or indirectly from the searches should be suppressed. The undersigned finds this argument unpersuasive.

The Fourth Amendment only applies to state action. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The Fourth Amendment's protection against unreasonable searches and seizures "is wholly inapplicable to a search or seizure . . . effected by a private individual not acting as an agent of the Government." *Id*. Defendant argues that Google, in reporting

to the NCMEC, was effectively acting as a government deputy in an anti-child pornography program and, therefore, qualifies as a government agent for purposes of the Fourth Amendment. The undersigned disagrees. In reporting the images found, Google was simply fulfilling its obligation under 18 U.S.C. § 2258A to report actual knowledge of any facts or circumstances involving child pornography. In another case discussing internet service providers' duties under § 2258A, the Eighth Circuit Court of Appeals concluded that "[a] reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013).[1] Google is a private, for profit entity. It complied with its statutory duty to report violations of child pornography laws. Google did not become a state actor by providing the reports required by law. Therefore, Defendant's request for suppression of evidence should be denied.

IT IS HEREBY RECOMMENDED to Senior District Court Judge Lyle Strom that Defendant's Motion (filing 33) be denied in its entirety.

A party may object to a magistrate judge's order by filing an objection within fourteen (14) days after being served with a copy of the findings and recommendation. Failure to timely object may constitute a waiver of any objection.

DATED September 9, 2015.

BY THE COURT:

S/ F.A. Gossett
United States Magistrate Judge

---

[1] Defendant argues that the United States Supreme Court's ruling in *Riley v. California*, 134 S.Ct. 2473 (2014), where the Court found that law enforcement needs a warrant before they can search the content of an individual's cell phone, indicates a change in the way the Supreme Court views digital privacy. However, the Supreme Court's ruling in *Riley* was within the context of law enforcement conducting searches incident to an arrest. It is distinguishable from the situation presented here–involving a private entity acting in accordance with a statutorily imposed duty. The *Riley* decision does not impact the *Stevenson* ruling's application to this case.